



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/008,053	11/09/2001	Matthew Hur	50325-0590	2815
29989	7590	04/10/2006	EXAMINER: SHIFERAW, ELENI A	
HICKMAN PALERMO TRUONG & BECKER, LLP 2055 GATEWAY PLACE SUITE 550 SAN JOSE, CA 95110			ART UNIT 2136	PAPER NUMBER

DATE MAILED: 04/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/008,053

Applicant(s)

HUR, MATTHEW

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 January 2006.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4,8-10,13-20 and 23-32 is/are pending in the application.
- 4a) Of the above claim(s) 3,5-7,11,12,21 and 22 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,4,8-10,13-20 and 23-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01/17/2006 has been entered.

Claim Rejections - 35 USC § 112

2. Claims 1, 8, 18, and 30-32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "longer-lived symmetric key" and "shorter-lived symmetric key" in independent claims 1, 8, 18, and 30-32 are a relative term which renders the claim indefinite. The terms "longer-lived symmetric key" and "shorter-lived symmetric key" are not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. On paragraph 0097 of the Applicant's disclosure "longer-lived symmetric key" and "shorter-lived symmetric key" are stated in terms of lifetime of the keys. However "longer-lived symmetric key" and "shorter-lived symmetric key" in the claims are not defined and it could introduce a different meaning for example, long and/or short keys in size. Applicant is advised to define "longer-lived symmetric key" and "shorter-lived symmetric key" in the claims to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 8, 18, and 30-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis WO 99/17495 in view of Lotspiech et al. Pub. No.: US 2002/0147906 A1 and Bruce Schneier 1996.

Regarding claims 1, 8, 18, and 30-32, Davis teaches a method/medium/apparatus of registering a non-configured network device in a telecommunication network (fig. 5), the method comprising the computer-implemented steps of:

providing trusted information (unique identifier of first device) to a trusted device registration service (an administrative entity) that certifies that the first device is a known device within a security realm and receiving in response, a registration service identifier that identifies an administrative entity to the first device (page 7 lines 10-15);

creating and storing device public key associated with the first device in a secure data repository that is accessible by the administrative entity (page 7 lines 15-page 8 lines 9);

authenticating the first device to the administrative entity by sending a message from the first device to the administrative entity that is encrypted using the device public key (page 8 lines 10-page 9 lines 12);

registering the first device in the network at the trusted device registration service (fig. 5-6);

receiving a message from the first device that requests network services (page 8 lines 26-31);

authenticating the first device (page 9 lines 1-12);

Davis fails to teach wherein:

wherein the trusted device registration service provides the first device with a longer-lived

symmetric key;

wherein the message from the first device contains the longer-lived symmetric key authenticating the first device based on the longer-lived symmetric key;

generating and providing a shorter-lived symmetric key to the first device based on authenticating the longer-lived symmetric key;

However Lotspiech discloses generating and providing a longer-lived symmetric session key and shorter-lived symmetric session key (par. 0014 and 0046):

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Lotspiech within the system of Davis because it would be difficult for intruders to determine the short-lived session key. One would have been motivated to do so because it would have secure communication by shortening the lifetime of the session key used to encrypt session between users.

Davis and Lotspiech fail to disclose the steps wherein:

receiving a request from a second network packet routing device to obtain a session key for secure communications between the second device and the first device, wherein the second device sends the request in response to receiving a request from the first device to obtain a session key on behalf of both the first device and the second device;

authenticating the request from the second device based on authenticating the shorter-lived symmetric key of the first device, wherein the request from the second device includes the shorter-lived symmetric key of the first device; and generating and providing a symmetric session key to the second device for use in subsequent secure peer-to-peer communications between the first device and the second device, wherein the first device obtains the symmetric session key from the second device without communication of the first device to a key management service or authoritative authentication service.

However Schneier discloses:

receiving a request from a second network packet routing device to obtain a session key for secure communications between the second device and the first device, wherein the second device sends the request in response to receiving a request from the first device to obtain a session key on behalf of both the first device and the second device (fig. 24.1);

authenticating the request from the second device based on authenticating the shorter-lived symmetric key of the first device, wherein the request from the second device includes the shorter-lived symmetric key of the first device (page 567-570); and

generating and providing a symmetric session key to the second device for use in subsequent secure peer-to-peer communications between the first device and the second device, wherein the first device obtains the symmetric session key from the second device without communication of the first device to a key management service or authoritative authentication service (pages 569-570).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Schneier's within the combination method of Davis and Lotspiech because it would have a secure communication between users.

5. Claims 1-5, 8-10, 13-20, 23-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sprunk et al. (Sprunk, Pub. No.: US 2005/0027985 A1) in view of Ganesan (Patent Number: 5,737,419), and Davis WO 99/17495.

As per claim 1 Sprunk teaches a method of registering a non-configured network device in a telecommunications network, the method comprising the computer-implemented steps of:

receiving a message from a first non-configured network device that requests network services (Sprunk Fig. 3 No. 310, page 3 par. 0043 lines 6-10, and page 5 par. 5 lines 1-3);

authenticating the first device based on a longer-lived symmetric key received from the first device (Sprunk page 2 par. 0033);

Art Unit: 2136

generating and providing a shorter-lived symmetric key to the first device based on authenticating the longer-lived symmetric key (Sprunk Fig. 3 No. 320; key validity period);

receiving a request from a second network packet routing device to obtain a session key for secure communications between the second device and the first device (Sprunk page 1 lines 12-20, and page 3 par. 0043);

generating and providing a symmetric session key to the second device for use in subsequent secure peer-to-peer communications between the first device and the second device without communication of either the first device or second device to a key management service or authoritative authentication service (Sprunk page 3 par. 0042);

registering the first device in the network at a trusted device registration service (Sprunk page 4 par. 0055, 0106-0116, and Fig. 5A,B; registering non-configured CTAs at HFC of IP telephony network/controller);

authenticating the first device to the trusted device registration service (par. 0011 lines 11-18, 0043, 0047-0051, and 0055);

providing trusted information to the trusted device registration service registration service that certifies that the first device as a known device within a security realm (0055, 0106-0116, and Fig. 5A,B; signed certificate from manufacturer and/or network operator); and

providing information identifying the device registration service to the first device for use in obtaining the longer-lived symmetric key (0105, 0055, and 0067; manufacturer generated lifetime certificate to CTAs).

Sprunk does not explicitly teach the shorter-lived symmetric key.

However Ganesan teaches the shorter-lived symmetric key (Ganesan col. 5 lines 2-7).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Ganesan within the system of Sprunk because the damage an attacker can cause by learning the short-lived key is significantly less than the damage which might be caused by compromise of long term key. (Ganesan col. 5 lines 2-7).

Sprunk and Ganesan fail to explicitly disclose configuring a non-configured network device as argued.

However Davis discloses configuring a non- configured network device as argued (abstract).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Davis within the combination system of Sprunk and Ganesan because it would it is well know to configure a non-configured device in a network (abstract).

As per claims 8, 18, and 30-32, Sprunk teaches a method/medium/apparatus for distributing cryptographic keys in a data network, comprising:

- a network packet routing interface that is coupled to the data network for receiving one or more packet flows therefrom (Sprunk page 1 par. 0012);

- a processor (Sprunk Fig. 2A No. 222);

- one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

- providing a registration service identifier that identifies an administrative entity to a first device and providing a unique identifier of the first device to the administrative entity (Sprunk page 5 par. 0067);

- associating a device private key in a secure data repository that is accessible by the administrative entity (Sprunk page 4 par. 0055);

- establishing a longer-lived symmetric key for the first device (Sprunk Fig. 3 No. 320, and page 5 par. 0068; key validity period);

- authenticating the first device based on receiving the longer-lived symmetric key from the first device (Sprunk page 2 par. 0033, and page 5 par. 0068; authenticating CTAs based on CTA request that has manufacturer certificate);

receiving a request from a second network routing device to obtain a session key for secure communications among the second device and the first device (Sprunk page 1 lines 12-20, and page 3 par. 0043);

generating and providing a symmetric session key to the second device for use in subsequent secure peer-to-peer communications between the first device and the second device without communication of either the first device or second device to a key management service or authoritative authentication (Sprunk page 3 par. 0042);

registering the first device in the network at a trusted device registration service (page 4 par. 0055, 0106-0116, and Fig. 5A,B; registering non-configured CTAs at HFC of IP telephony network/controller);

authenticating the first device to the trusted device registration service (par. 0011 lines 11-18, 0043, 0047-0051, and 0055);

generating trusted information for the trusted device registration service that certifies that the first device as a known device within a security realm (0055, 0106-0116, and Fig. 5A,B; signed certificate from manufacturer and/or network operator); and

generating information identifying the device registration service to the first device for use in obtaining the longer-lived symmetric key (0105, 0055, and 0067; manufacturer generated lifetime certificate to CTAs).

Sprunk does not explicitly teach the shorter-lived symmetric key.

However Ganesan teaches the shorter-lived symmetric key (Ganesan col. 5 lines 2-7).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Ganesan within the system of Sprunk because the damage an attacker can cause by learning the short-lived key is significantly less than the damage which might be caused by compromise of long term key. (Ganesan col. 5 lines 2-7).

Sprunk and Ganesan fail to explicitly disclose configuring a non-configured network device as argued.

However Davis discloses configuring a non- configured network device as argued (abstract).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Davis within the combination system of Sprunk and Ganesan because it would it is well know to configure a non-configured device in a network (abstract).

As per claim 2, Sprunk, Ganesan, and Davis teach all the subject matter as described above. In addition, Ganesan teaches a method, wherein the shorter-lived symmetric key is encapsulated in a ticket that includes data identifying a specified lifetime of the shorter-lived symmetric key (Ganesan col. 4 lines 56-col 5 lines 2-7). The rational for combining are the same as claim 1 above.

As per claim 3, Sprunk, Ganesan, and Davis teach all the subject matter as described above. In addition, the combination of Sprunk and Ganesan teach a method, further comprising the steps of receiving, at the second device, a request from the first device to obtain a session key on behalf of both the first device and second device, wherein the request includes the shorter-lived symmetric key of the first device (Sprunk page 5 par. 0071, and Ganesan col. 5 lines 2-7).

As per claim 4, Sprunk, Ganesan, and Davis teach all the subject matter as described above. In addition, Sprunk teaches a method, wherein the subsequent secure communications comprise successive symmetric encryption and decryption operations using the symmetric session key, and wherein the first device and second device carry out the subsequent secure communications without contact with a key management service or registration service (Sprunk page 2 par. 0031, page 1 par. 0011 lines 12-20).

As per claim 5, Sprunk, Ganesan, and Davis teach all the subject matter as described above. In addition, Sprunk teaches a method, further comprising the steps of:

receiving a request from a first device that wishes to communicate securely with a second device to register with a trusted registration service (Sprunk Fig. 1 No. 310);
authenticating the first device (Sprunk page 2 par. 0033); and
in response to authenticating the first device, providing a longer-lived symmetric key to the first device (Sprunk Fig. 3 No. 320; key validity period).

As per claim 7, Sprunk, Ganesan, and Davis teach all the subject matter as described above. In addition, Sprunk teaches a method, further comprising the steps of:

providing trusted information to the trusted registration service that certifies that the first device as a known device within a security realm (Sprunk page 5 par. 0067, and fig. 3 No. 310); and
providing information identifying the registration service to the first device for use in obtaining the longer-lived symmetric key (Sprunk Fig. 3 No. 320).

As per claims 9 and 19, Sprunk, Ganesan, and Davis teach all the subject matter as described above. In addition, Sprunk teaches a method/medium/apparatus, teaches a method wherein the step of associating a device private key with a data repository comprises the steps of generating a public key pair comprising a device public key and a device private key and storing the device private key in a database or directory that is accessible to the administrative entity (Sprunk page 4 par. 0055).

As per claims 10 and 20, Sprunk, Ganesan, and Davis teach all the subject matter as described above. In addition, Sprunk teaches a method/medium/apparatus, wherein the step of associating a device private key with a data repository comprises the steps of generating a public key pair comprising a device public key and a device private key and registering the device private key with a certification authority that is accessible to the administrative entity (Sprunk page 4 par. 0055).

As per claims 13 and 23, Sprunk, Ganesan, and Davis teach all the subject matter as described above. In addition, Sprunk teaches a method/medium/apparatus, wherein generating trusted information for the trusted registration service comprises the steps of creating and storing an association of a unique identifier of the first device and the device public key in a secure database that is accessible to the registration service, and providing the unique identifier from the first device to the registration service (Sprunk page 4 par. 0055, and page 5 par. 0068).

As per claims 14 and 24, Sprunk, Ganesan, and Davis teach all the subject matter as described above. In addition, Sprunk teaches a method/medium/apparatus, wherein establishing a longer-lived symmetric key comprises the steps of:

- generating the longer-lived symmetric key (Sprunk Fig. 3 No. 320);

- encrypting the longer-lived symmetric key using the device public key (Sprunk Fig. 3 No. 320, and page 3 par. 0044);

- encapsulating the encrypted longer-lived symmetric key in a device registration ticket (Sprunk page 3 par. 0044 lines 1-3); and

- sending the device registration ticket to the device (Sprunk page 5 par. 0071 and page 3 par. 0044-0045).

As per claims 15 and 25, Sprunk, Ganesan, and Davis teach all the subject matter as described above. In addition, Sprunk teaches a method/medium/apparatus, wherein encapsulating the encrypted key comprises encapsulating the encrypted longer-lived symmetric key with policy information in the device registration ticket, wherein the policy information defines a validity interval of the encrypted longer-lived symmetric key (Sprunk Fig. 3 No. 320, and page 3 par. 0046).

Art Unit: 2136

As per claims 16 and 26, Sprunk, Ganesan, and Davis teach all the subject matter as described above. In addition, the combination of Sprunk and Ganesan teach a method/medium/apparatus, wherein generating and providing a short-term symmetric key to the first device includes the steps of encapsulating the short-term symmetric key in a short-term ticket granting ticket with associated policy information (Sprunk page 4 par. 0055, and Ganesan col. 4 lines 56-col 5 lines 2-7). The rationale for combining are the same as claim 8 above.

As per claims 17 and 27, Sprunk, Ganesan, and Davis teach all the subject matter as described above. In addition, the combination of Sprunk and Ganesan teach a method/medium/apparatus, wherein the step of receiving a request from a second device to obtain a session key for secure communications among the second device and the first device comprises the steps of:

- receiving a first short-term ticket granting ticket that includes the short-term symmetric key of the first device (Ganesan col. 23 lines 60-col. 24 lines 13, and col. 5 lines 2-7);

- receiving a second short-term ticket granting ticket that includes the short-term symmetric key of the second device (Ganesan col. 23 lines 60-col. 24 lines 13, and col. 5 lines 2-7);

- decrypting the first and second short-term ticket granting tickets based on respective first and second shared secret keys (Sprunk page 4 par. 0055, and Ganesan col. 4 lines 56-col 5 lines 2-7);

- authenticating the short-term symmetric keys of the first device and second device based on the respective first and second shared secret keys (Sprunk page 4 par. 0055, and Ganesan col. 4 lines 56-col 5 lines 2-7); and

- generating and providing a symmetric session key to the second device for use in subsequent secure peer-to-peer communications between the first device and the second device without communication of either the first device or second device to a key management service or authoritative authentication service (Ganesan col. 8 lines 21-32, and Sprunk page 3 par. 0042). The rationale for combining are the same as claim 8 above.

Conclusion


6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 20030105812 A1, US 20030065731 A1, US 20030046398, and US 5479514. (*Peer to peer communication session request to key server/other peer is very well known at the time of the invention*).

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.


March 31, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

 4/2/06